

AMENDMENTS TO THE CLAIMS

Please amend the claims as indicated in the following complete listing of claims.

1. (Currently Amended) An authentication system, said authentication system comprising:

a portable card terminal, including:

first identification information storage means having a first identification information ~~pre-stored~~ stored therein for discriminating said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

operating means for inputting a second identification information associated with said first identification information,

encryption means for encrypting the second identification information input by said operating means based on ~~an~~ encryption key information, and

first communication means for communication with ~~said~~ an authentication device, wherein said communication includes transmitting the first identification information to said authentication device and receiving said encryption key information from the authentication device in response to transmitting the first identification information;

~~an~~ said authentication device, provided independently of said portable card terminal for communication with said portable card terminal, the authentication device including:

second identification information storage means for storage of the first identification information and the second identification information therein,

encryption key information generating means for generating said encryption key information, wherein said encryption key information comprises a random number, and wherein said encryption key information is generated in response to receiving the first identification information from said portable terminal,

second communication means for communication with said portable card terminal, and
comparator authentication means for comparing and authenticating the second identification information encrypted by said encryption means based on said encryption key information;

wherein said portable card terminal encrypts the second identification information input from said operating means, based on said encryption key information received from said authentication device, the so-encrypted second identification information is transmitted through said first communication means to said authentication device; and

wherein, in said authentication device, the encrypted second identification information received through said second communication means and the second identification information stored by said second identification information storage means are compared to each other based on said encryption key information ~~by way of performing~~ to perform the authentication.

2. (Previously Presented) The authentication system according to claim 1 wherein said authentication device includes:

decoding means for decoding the second identification information encrypted by said encrypting means based on said encryption key information,

said authentication device decoding the received encrypted second identification information based on said encryption key information, said authentication device comparing the

decoded second identification information to the second identification information stored in said second identification information storage means, by way of performing the authentication.

3. (Previously Presented) The authentication system according to claim 2, wherein said second identification information is a password of a service user made up of a preset letter string or a preset string of numerical figures,

4. (Previously Presented) The authentication system according to claim 3 for authenticating the service user to whom preset services are offered from a service provider in a credit sale system, an inter-account instant payment system and in E-commerce carried out over a preset network, wherein

said portable card terminal is a card-shaped portable terminal issued by said service provider to said service user,

said authentication device being contained in a host computer in which said service provider authenticates usage by said service user, and

said service user being authenticated by said authentication device authenticating said portable card terminal and that said service user is a true owner of the portable card terminal.

5. (Previously Presented) The authentication system according to claim 4, wherein said first and second communication means are wireless communication means.

6. (Currently Amended) The authentication system according to claim 4, wherein said portable card terminal includes a transient storage means in which the second identification information is stored transiently.

7. (Previously Presented) The authentication system according to claim 6, wherein said transient storage means stores the second identification information input by said operating means until authentication of said portable card terminal by said authentication device.

8. (Previously Presented) The authentication system according to claim 6, wherein said second identification information stored in said transient storage means is erased every preset time interval.

9. (Previously Presented) The authentication system according to claim 6, wherein said operating means in said portable card terminal includes means for erasing the second identification information stored in said transient storage means.

10. (Previously Presented) The authentication system according to claim 4, wherein said operating means in said portable card terminal includes a plurality of input units for letters or numerical figures for inputting said second identification information, and wherein the arraying positions of said letter input units are variable.

11. (Previously Presented) The authentication system according to claim 10, wherein the arraying positions of said letter inputting units are varied prior to the inputting of said second identification information.

12. (Previously Presented) The authentication system according to claim 10, wherein said operating means in said portable card terminal includes a display unit for displaying letters and a selection unit for selecting the letters displayed on said display unit, and wherein the second identification information input by said operating means is made up by a string of letters selected by said selection unit from among plural letters sequentially displayed on said display unit.

13. (Currently Amended) An authentication method in which a portable card terminal is authenticated by an authentication device provided independently of said portable card terminal, said method comprising

an operating step of inputting a second identification information associated with a first identification information that discriminates said portable card terminal and that is ~~pre-stored~~ stored in a first identification information storage means of said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

an encryption key information generating step of generating an encryption key information by transmitting the first identification information from the portable card terminal to the authentication device, and receiving said encryption key information from the authentication device in response to transmitting the first identification information, wherein said encryption

key information is generated by the authentication device in response to receiving the first identification information from the portable card terminal,

an encrypting step of encrypting the second identification information input at said operating step, based on the encryption key information generated in said encryption key information generating step, and

a comparison authentication step of comparing the second identification information encrypted in said encrypting step to the second identification information as stored in a second identification information storage means to perform the authentication.

14. (Previously Presented) The authentication method according to claim 13 further comprising

a decoding step of decoding the second identification information, encrypted in said encrypting step, based on said encryption key information,

the encrypted second identification information being decoded in said decoding step based on said encryption key information, and the decoded second identification information being compared to the second identification information stored in said second identification information storage means by way of performing the authentication.

15. (Previously Presented) The authentication method according to claim 14, wherein the encryption key information comprises a random number.

16. (Previously Presented) The authentication method according to claim 15 for authenticating a service user to whom preset services are offered from a service provider in a credit sale system, an inter-account instant payment system and in E-commerce carried out over a preset network, wherein

said portable card terminal is a card-shaped portable terminal issued by said service provider to said service user,

said authentication device being an authentication device contained in a host computer in which said service provider authenticates usage by said service user, and

said service user being authenticated by said authentication device authenticating said portable card terminal and that said service user is a true owner of the portable card terminal.

17. (Previously Presented) The authentication method according to claim 16, wherein said portable card terminal and the authentication device are interconnected by wireless communication means.

18. (Previously Presented) The authentication method according to claim 16, wherein said portable card terminal includes a transient storage step of transiently storing the second identification information.

19. (Previously Presented) The authentication method according to claim 18, wherein said transient storage step stores the second identification information input in said operating step until authentication of said portable card terminal by said authentication device.

20. (Previously presented) The authentication method according to claim 18, wherein said second identification information stored in said transient storage step is erased every preset time interval.

21. (Previously presented) The authentication method according to claim 18, wherein said operating step includes a step of erasing the second identification information stored in said transient storage step.

22. (Previously Presented) The authentication method according to claim 16, wherein said operating step includes a letter inputting step of inputting said second identification information, and wherein the second identification information is input in said letter inputting step via a plurality of letter inputting units the arraying positions of which are variable.

23. (Previously Presented) The authentication method according to claim 22, wherein the arraying positions of said plural letters in said letter inputting step are varied prior to inputting of said second identification information.

24. (Previously Presented) The authentication method according to claim 22, wherein said operating step includes a display step of displaying letters and a selection step of selecting the letters displayed in said display step, and wherein the second identification information input

by said operating step is made up by a string of letters selected in said selection step from among plural letters sequentially displayed in said display step.

25. (Withdrawn) An encryption key inputting device in which a string of a preset number of letters comprised of a combination of letters included in a preset group of letters is a letter string for authentication, said device comprising

display means for irregularly displaying the letters included in said preset group of letters, and selection means for selecting said letter string for authentication from among the letters irregularly displayed on said display means.

26. (Withdrawn) The encryption key inputting device according to claim 25, wherein said preset group of letters is ten numerical figures from 0 to 9.

27. (Withdrawn) The encryption key inputting device according to claim 25, wherein said display means irregularly displays said numerical figures in optional positions in said display means.

28. (Withdrawn) The encryption key inputting device according to claim 25, wherein said display means displays said numerical figures one-by-one in an irregular sequence.

29. (Withdrawn) The encryption key inputting device according to claim 25, wherein said display means displays the pre-entered numerical figures from 0 to 9 or the vicinity thereof by emitting light thereat to indicate respective numerical figures.

30. (Withdrawn) An encryption key inputting method in which a string of a preset number of letters comprised of a combination of letters included in a preset group of letters is a letter string for authentication, said method comprising

a displaying step of irregularly displaying the letters included in said preset group of letters, and

a selection step of selecting said letter string for authentication from among the letters irregularly displayed in said display step.

31. (Withdrawn) The encryption key inputting method according to claim 30, wherein said preset group of letters is ten numerical figures from 0 to 9.

32. (Withdrawn) The encryption key inputting method according to claim 30, wherein said display step irregularly displays said numerical figures in optional positions in said display step.

33. (Withdrawn) The encryption key inputting method according to claim 30, wherein said display step displays said numerical figures one-by-one in an irregular sequence.

34. (Withdrawn) The encryption key inputting method according to claim 30, wherein said display step displays the pre-entered numerical figures from 0 to 9 or the vicinity thereof by emitting light thereat to indicate respective numerical figures.

35. (Currently Amended) A portable card terminal authenticated by an authentication device, comprising,

first identification information storage means for storing a first identification information for discriminating said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

operating means for inputting a second identification information associated with said first identification information,

communication means for communication with said authentication device wherein said communication including transmitting the first identification information from the portable card terminal to the authentication device, and receiving encryption key information from the authentication device in response to transmitting the first identification information, and

encrypting means for encrypting the second identification information input by said operating means based on ~~an~~ said encryption key information received from said authentication device, wherein said encryption key information is generated by the authentication device in response to receiving the first identification information from the portable card terminal.

36. (Previously Presented) The portable card terminal according to claim 35, wherein said encryption key information comprises a random number.

37. (Previously Presented) The portable card terminal according to claim 35, wherein the portable card terminal is issued to a service user by a service provider to offer preset services for said service user in a credit sale system, an inter-account instant payment system and E-commerce carried out over a preset network and is in the form of a card.

38. (Previously Presented) The portable card terminal according to claim 37, wherein said communication means are wireless communication means.

39. (Previously Presented) The portable card terminal according to claim 37, wherein said portable card terminal includes transient storage means in which the second identification information is stored transiently.

40. (Previously Presented) The portable card terminal according to claim 39, wherein said transient storage means stores the second identification information input by said operating means until authentication of said portable card terminal by said authentication device.

41. (Previously Presented) The portable card terminal according to claim 39, wherein said second identification information stored in said transient storage means is erased every preset time interval.

42. (Previously Presented) The portable card terminal according to claim 39, wherein said operating means in said portable card terminal includes means for erasing the second identification information stored in said transient storage means.

43. (Previously Presented) The portable card terminal according to claim 37, wherein said operating means includes a plurality of letter inputting means for inputting said second identification information, and wherein the arraying positions of said letter inputting units are variable.

44. (Previously Presented) The portable card terminal according to claim 43, wherein the arraying positions of said plural letters in said letter inputting means are varied prior to the inputting of said second identification information.

45. (Previously Presented) The portable card terminal according to claim 43, wherein said operating means includes a display unit for displaying letters and a selection unit for selecting the letters displayed in said display unit, and wherein the second identification information input by said operating means is made up by a string of letters selected in said selection unit from among plural letters sequentially displayed on said display unit.

46. (Currently Amended) An authentication system made up by a portable card terminal and an authentication device provided independently of said portable card terminal for communication with said portable card terminal, said authentication system comprising:

said portable card terminal, including

first identification information storage means having a first identification information ~~pre-stored~~ stored therein for discriminating said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

operating means including display means for irregularly displaying letters included in a group of letters and selection means for selecting the letters making up a second identification information from among the letters irregularly displayed on said display means, said operating means inputting the second identification information associated with said first identification information,

encryption means for encrypting the second identification information input by said operating means based on an encryption key information, and

first communication means for communication with said authentication device, wherein said communication includes transmitting the first identification information to said authentication device and receiving said encryption key information from the authentication device in response to transmitting the first identification information;

said authentication device, including

second identification information storage means having the first identification information and the second identification information stored therein,

encryption key information generating means for generating said encryption key information, wherein said encryption key information is generated in response to receiving the first identification information from said portable terminal,

second communication means for communication with said portable card terminal, and comparator authentication means for comparing the second identification information encrypted by said encryption means to the second identification information stored in the second identification information storage means; wherein

said portable card terminal encrypts the second identification information input from said operating means, based on said encryption key information received from said authentication device through said first communication means, and the so-encrypted second identification information is transmitted through said first communication means to said authentication device; and

wherein, in said authentication device, the encrypted second identification information received through said second communication means and the second identification information stored by said second identification information storage means are compared to each other based on said encryption key information ~~by way of performing~~ to perform the authentication.